

Forum:[Hack Forums](#)

Thread: [Improving the Bug Bounty Program: Guidelines, Communication & Avoiding Accidental Ban](#)

Disarray"" - June 16, 2023, 4:35 pm

Recently, I experienced a ban that I believe resulted from miscommunication and my lack of experience in hunting on smaller websites. I didn't fully consider how my actions could be perceived as those of a malicious actor especially on a smaller site like this where it's easy to watch someone. I'm grateful to Omniscient for taking the time to listen to my perspective and understanding my point of view, and lifting my ban.

I'd like to propose some modifications to the bug bounty program (<https://hackforums.net/showthread.php?tid=5259373>) to avoid what happened to me, and generally improve the policy as a whole.

1. Clearer communication guidelines: Bug hunters should inform the owner before starting their testing, either via a private message or any other preferred communication channel. This will help avoid misunderstandings and accidental bans. (This is not a normal policy, but seems to be wanted/needed)
2. Identification of bug hunters: Bug hunters should include a specific identifier in their hf signature, or as an HTTP header (e.g., x-bughunter: @hackforum_username). This will help staff members recognize bug hunters and reduce the risk of accidental bans.
3. Testing limitations: I think the policy could be more clear on what is, or is not allowed. Automated scanning is already disallowed, but social engineering allowed? Open redirects, what about self XSS? I think the policy should be more clear on what is, or is not allowed.
4. Reporting process: The policy should provide a clear and structured reporting process for bug hunters to follow when submitting their findings. This can include a template for reporting vulnerabilities, the expected response time from the program owner, and any additional information required for verification and patching. Generally it includes the following: Summary, Description, Steps to Reproduce, Impact, Proof of Concept, and sometimes Remediation suggestions.
5. Scope clarification: The policy should clearly define the scope of the program, including the specific systems, applications, and features that are in scope for testing. I found some subdomains, and I wasn't sure if they were in scope or not. I think the policy should be more clear on what is, or is not allowed.
6. Rewards for severity level: In bug bounty programs, there are typically five main severity levels, as seen on platforms like HackerOne: Informative, Low, Medium, High, and Critical. To encourage bug hunters to focus on finding more significant vulnerabilities, the program should offer tiered rewards based on the severity level of the reported issue. Here's a brief overview of each level and examples of vulnerabilities that may fall under each category:

- Informative: Issues that do not pose a direct security risk but may provide useful information for improving the overall security posture. Examples include best practice recommendations, outdated software versions, or misconfigurations that do not lead to direct exploitation.

- Low: Vulnerabilities that pose a limited security risk, often requiring user interaction or specific

conditions to be exploited. Examples include open redirects, self-XSS, CSS injection, and HTML injection.

- Medium: Issues that present a moderate security risk, often allowing an attacker to access information that shouldn't be exposed or perform unauthorized actions that aren't that dangerous.

- High: Vulnerabilities that pose a significant security risk, often allowing an attacker to compromise user accounts, access sensitive data, or perform critical actions. Examples include stored XSS, Cross-Site Request Forgery (CSRF) on sensitive actions, SQL Injection, and some less severe Remote Code Execution (RCE) vulnerabilities.

- Critical: Issues that present an extreme security risk, often allowing an attacker to fully compromise the system, execute arbitrary code, or access highly sensitive data. Examples include severe RCE vulnerabilities, SQL Injection leading to full database access, and critical authentication bypass vulnerabilities.

Currently, it seems the only vulnerability that will be accepted is one that can reveal the hashed password of the admin. I think just adding more severity levels and broadening the scope would be nice, even if it's very low rewards. Hell, I think even some bytes or a hf award would incentivize people to the report bugs.

Omniscient - June 16, 2023, 5:04 pm

Suppose I can update that thread with some additional information.

Disarray"" - June 16, 2023, 10:08 pm

Sounds good, looking forward to it

source - June 17, 2023, 9:15 am

Glad to see you got your account back. Also glad to see some updates on the bbp

Omniscient - June 17, 2023, 1:21 pm

<https://hackforums.net/showthread.php?tid=6244277>

That should clarify.

Disarray"" - June 17, 2023, 1:35 pm

(Jun 17, 2023 01:21 PM)Omniscient Wrote: [\[CITE\]](#)
<https://hackforums.net/showthread.php?tid=6244277>

That should clarify.

Thanks! looks good